## 探测行为识别技术

### 设备实体探测行为识别

目前,最为主流的设备探测技术依然是基于指纹实现的,如Shodan、Zoomeye、Censys以及各类漏洞扫描产品,基本原理是对目标设备进行网络扫描,根据响应包中的多个字段信息构造设备指纹,如开放端口号、会话方式及协议等,同指纹库进行匹配,确定探测的设备类别。因此,通过识别指纹探测行为,可以有效识别相应设备的探测行为。

为了细粒度地识别设备探测行为,可根据设备指纹库将设备分类,基于不同类别设备的探测方法的差异性,识别探测数据包。根据网络空间大多数设备已有相应的分类命名规则,确定每类设备的网络扫描方法,识别网络扫描数据包的格式,提取特征,归纳聚合,建立设备探测行为指纹库。

扫描程序发出的请求数据包和常规请求数据包之间往往存在内容上的差异,这些差异可以被用作识别探测行为的指纹。例如,Nmap在进行操作系统扫描时,发送的UDP数据包中默认使用字符“C”填充数据部分,而在ICMP数据包中使用“0”填充,同时,扫描时默认的TCP窗口大小字段固定为“1024”;Zmap在扫描时使用固定的IPID“54321”以及固定的窗口大小“65535”。针对部分未知类别的设备,通过深入分析设备探测行为的模式,将其与已知类别设备的探测行为模式相比较,采用相似性度量方法,将其归类为最相似的类别,从而识别针对该设备的探测行为。

### 应用服务探测行为识别

针对应用服务的探测主要有端口扫描和漏洞扫描。端口扫描是向目标系统发送探测数据包,旨在探测网络主机是否存在开放端口和其他可用服务;漏洞扫描是在端口扫描的基础上,将扫描结果同漏洞库数据进行匹配,进一步识别应用服务类型、版本等信息。

为了识别应用服务探测行为,首先应分析系统端口的开放状态,并且记录探测方访问应用服务时留下的信息,进而通过分析探测数据包、提取报文特征、建立数学模型、数据可视化等方式,并结合统计学方法、人工智能算法或其他启发式方法识别探测行为。

为了识别应用层的探测行为,我们可以通过HTTP的状态码、URL长度、User-Agent字段等特征来区分探测程序发出的请求和正常请求。例如,Web漏洞扫描器Awvs(AcunetixWebVulnerabilityScanner)在请求的URL、Headers、Body等字段包含了“by\_wvs”、“acunetix\_wvs\_security\_test”等能代表自己的特征字符串;Sqlmap在User-Agent中包含了“sqlmap”这个特征字符串。

### 局限性

设备实体探测和应用服务探测行为识别依赖于对扫描工具的指纹构建,但通常有经验的攻击方会基于开源的扫描工具进行二次开发,刻意改变默认字段、请求负载等指纹特征,从而使得原有的指纹信息失效。扫描工具的行为模式、流量统计信息等特征也在时刻变化,加大了统计学方法、人工智能算法或其他启发式方法的识别难度。

### 流量行为分析

针对以上局限性，我们可以分析流量行为，总结出不同扫描器或者搜索引擎的扫描行为规律，进而确定其扫描行为。